

PH <sup>US</sup> 010314W0	MAT. DOSSIER
------------------------------	-----------------

①9 RÉPUBLIQUE FRANÇAISE

①1 N° de publication :

2 781 076

INSTITUT NATIONAL  
DE LA PROPRIÉTÉ INDUSTRIELLE

(à n'utiliser que pour les  
commandes de reproduction)

②1 N° d'enregistrement national :

98 08863

PARIS

⑤1 Int Cl<sup>7</sup> : G 08 C 19/00, H 04 B 3/00

## ①2 DEMANDE DE BREVET D'INVENTION

A1

②2 Date de dépôt : 09.07.98.

③0 Priorité :

⑦1 Demandeur(s) : VALEO SECURITE HABITACLE  
Société anonyme — FR.

④3 Date de mise à la disposition du public de la  
demande : 14.01.00 Bulletin 00/02

⑦2 Inventeur(s) : AVENEL JEAN JACQUES.

⑤6 Liste des documents cités dans le rapport de  
recherche préliminaire : Se reporter à la fin du  
présent fascicule

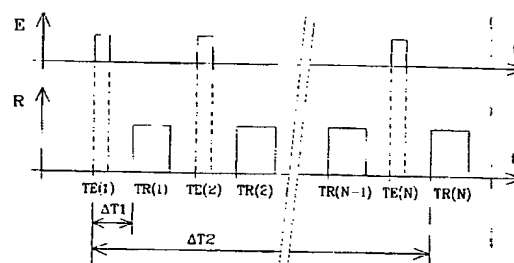
⑦3 Titulaire(s) :

⑥0 Références à d'autres documents nationaux  
apparentés :

⑦4 Mandataire(s) : VALEO MANAGEMENT SERVICES.

⑤4 **SYSTEME DE SECURITE POUR UN VEHICULE AUTOMOBILE COMPORTANT DES MOYENS DE MESURE DE LA DUREE D'UN ECHANGE DE DONNEES.**

⑤7 L'invention propose un système de sécurité pour un véhicule automobile, du type dans lequel, en vue de la délivrance d'une autorisation, le système procède à une opération d'identification au moyen de signaux électromagnétiques échangés à distance entre une centrale d'identification et un identifiant, du type dans lequel l'opération d'identification comporte une étape d'échange de données au cours de laquelle est exécutée au moins une boucle d'identification selon laquelle un signal d'interrogation est émis par la centrale vers l'identifiant qui émet en retour un signal de réponse en direction de la centrale, et du type dans lequel l'opération d'identification comporte une étape d'authentification du signal de réponse, caractérisé en ce que l'opération d'identification comporte une étape de contrôle de la durée de l'étape d'échange de données.



FR 2 781 076 - A1



L'invention concerne un système de sécurité pour un véhicule automobile comportant des moyens de mesure de la durée d'un échange de données.

L'invention se rapporte plus particulièrement à un système de sécurité pour un véhicule automobile, du type dans lequel, en vue de la délivrance d'une autorisation, le système procède à une opération d'identification au moyen de signaux électromagnétiques échangés à distance entre une centrale d'identification et un identifiant, du type dans lequel l'opération d'identification comporte une étape d'échange de données au cours de laquelle est exécutée, au moins une boucle d'identification selon laquelle un signal d'interrogation est émis par la centrale vers l'identifiant qui émet en retour un signal de réponse en direction de la centrale, et du type dans lequel l'opération d'identification comporte une étape d'authentification du signal de réponse.

On trouve de tels systèmes de sécurité par exemple dans les dispositifs de verrouillage des ouvrants d'un véhicule automobile.

Dans un tel dispositif, chaque ouvrant est muni d'une serrure qui est susceptible d'être commandée par une centrale d'antivol entre un état verrouillé et un état déverrouillé.

Pour provoquer le déverrouillage des serrures, l'utilisateur doit tout d'abord déclencher une opération d'identification. Ce déclenchement peut être réalisé par exemple à l'aide d'une télécommande, par appui sur un bouton de commande situé sur l'ouvrant, ou éventuellement grâce à un détecteur de présence qui est incorporé au véhicule, qui détecte l'arrivée d'une personne à proximité du véhicule et qui déclenche alors le processus d'identification.

Ainsi que cela est représenté sur la figure 1, l'opération d'identification est basée sur un échange de données entre la centrale d'antivol 10 incorporée au véhicule et un identifiant 12 porté par l'utilisateur qui est autorisé à utiliser ce véhicule. Cet identifiant 12 est par exemple un transpondeur électromagnétique qui, en réponse à un signal d'interrogation, émet un signal codé en direction de la centrale d'antivol.

Au cours d'une étape d'authentification, la centrale 10 vérifie que le code renvoyé par l'identifiant 12 correspond au code autorisé et, le cas échéant, la centrale d'antivol 10 délivre un signal d'autorisation qui provoque le déverrouillage des serrures et permet donc l'accès à l'habitacle du véhicule.

Généralement, les données échangées entre la centrale d'antivol 10 et l'identifiant 12 sont formées de signaux électromagnétiques à courte portée, c'est-à-dire que l'opération d'identification ne peut s'effectuer que lorsque l'identifiant 12, et donc la personne qui le porte, se trouve dans un rayon de quelques mètres autour du véhicule.

Un tel système présente donc en théorie, une grande fiabilité et assure un haut niveau de sécurité, notamment lorsque l'on utilise un identifiant 12 capable d'émettre, à chaque interrogation, un signal de réponse portant un code différent, ce qui évite la possibilité pour un malfaiteur d'enregistrer le signal codé et de le ré-émettre pour simuler la présence de l'identifiant 12.

Toutefois, on a illustré sur la figure 2, des moyens qui peuvent permettre à des malfaiteurs de contourner l'obstacle représenté par cette opération d'identification.

En effet, on a vu que, par construction, on cherchait à limiter la portée de transmission lors de l'échange de données entre la centrale d'antivol et l'identifiant pour ne permettre l'ouverture du véhicule que lorsque l'utilisateur autorisé se situe à proximité immédiate de celui-ci.

Cependant, il est apparu qu'il était possible à des malfaiteurs de simuler cette proximité de manière particulièrement discrète, sans qu'ils aient à s'emparer de l'identifiant ni qu'ils aient à connaître la nature ou le contenu des données échangées entre la centrale d'antivol 10 et l'identifiant 12.

En effet, il est possible d'augmenter artificiellement la portée de la transmission en interposant entre la centrale 10 et l'identifiant 12 deux relais, ou stations de relais 14, 16 autorisant une transmission selon une distance beaucoup plus longue.

On peut ainsi disposer un premier relais 14 à proximité du véhicule, et donc à proximité de la centrale 10. Lorsque la centrale 10 émet un signal d'interrogation, celui-ci est reçu par le premier relais 14 et il est ré-émis, sous la forme par exemple d'une onde hertzienne à haute fréquence dont la portée est relativement importante, en tous cas supérieure à quelques centaines de mètres. Le signal ré-émis par le premier relais 14 est alors reçu par le second relais 16 que l'on a préalablement disposé à proximité de l'identifiant 12 porté par l'utilisateur autorisé.

Ce second relais 16 ré-émet le signal qu'il reçoit du premier relais 14 sous la forme par exemple d'une onde hertzienne à basse fréquence identique à celle initialement émise par la centrale d'antivol

10. Ce signal provoque donc l'activation de l'identifiant 12, lequel émet alors son signal de réponse qui, à son tour, est susceptible d'être reçu par le second relais 16. Le second relais 16 ré-émet alors le signal de réponse, là encore sous la forme d'un signal électromagnétique à longue portée en direction du premier relais 14 qui transforme ce signal reçu en un signal identique à celui qui a été émis par l'identifiant 12.

La centrale d'antivol 10 reçoit alors, en provenance du premier relais 14 un signal qu'elle interprète comme provenant directement de l'identifiant 12 et qu'elle est apte à authentifier. Si le signal est authentique, le système de sécurité provoque la délivrance d'un signal d'autorisation permettant, entre autres, le déverrouillage des serrures.

On le voit, un tel dispositif permet donc de provoquer l'ouverture du véhicule sans qu'il n'y ait d'effraction visible et, surtout, sans que l'utilisateur autorisé ne s'en rende compte.

En effet, en pratique, les relais 14, 16 peuvent être agencés dans des malles portées par des malfaiteurs, l'un des malfaiteurs restant à proximité du véhicule tandis que l'autre malfaiteur suit l'utilisateur autorisé qui est par exemple en train de s'éloigner de son véhicule.

L'invention a donc pour objet de proposer une nouvelle conception d'un système de sécurité qui permette de rendre inefficace ces moyens de contourner l'opération d'identification effectuée par le système de sécurité.

Dans ce but, l'invention propose un système de sécurité pour un véhicule automobile, du type dans lequel, en vue de la délivrance d'une autorisation, le système procède à une opération d'identification au moyen de signaux électromagnétiques échangés à distance entre une centrale d'identification et un identifiant, du type dans lequel l'opération d'identification comporte une étape d'échange de données au cours de laquelle est exécutée au moins une boucle d'identification selon laquelle un signal d'interrogation est émis par la centrale vers l'identifiant qui émet en retour un signal de réponse en direction de la centrale, et du type dans lequel l'opération d'identification comporte une étape d'authentification du signal de réponse, caractérisé en ce que l'opération d'identification comporte une étape de contrôle de la durée de l'étape d'échange de données.

Selon d'autres caractéristiques de l'invention :

- l'étape de contrôle de la durée compare la durée entre l'émission par la centrale d'un signal d'interrogation et la réception par

la centrale du signal retour correspondant avec une durée prédéterminée;

l'étape d'échange de données comporte l'exécution d'une série de boucles successives d'identification, une boucle de rang supérieur n'étant exécutée qu'une fois achevée la boucle de rang immédiatement inférieur, et l'étape de contrôle de la durée compare la durée entre l'émission du signal d'interrogation d'une boucle de la série et la réception du signal de réponse d'une boucle de rang supérieur déterminé, avec une durée prédéterminée;

les signaux électromagnétiques échangés entre la centrale d'identification et l'identifiant sont, dans l'un au moins des sens de transmission, des signaux de faible portée.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description détaillée qui suit pour la compréhension de

laquelle on se reportera aux dessins annexés dans lesquels :

la figure 1 est une vue schématique illustrant l'échange de données entre la centrale d'antivol et l'identifiant lorsque les deux sont à proximité l'un de l'autre;

la figure 2 est une vue similaire à celle de la figure 1 qui illustre l'échange de données lorsque deux relais sont interposés entre la centrale d'antivol et l'identifiant pour permettre l'échange de données lorsque ces deux éléments sont éloignés l'un de l'autre d'une distance supérieure à la portée nominale ;

la figure 3 est un graphe sur lequel on a porté en abscisse le temps et en ordonnée d'une part les moments d'émission par la centrale d'antivol du signal d'interrogation, et d'autre part les moments de réception par la centrale d'antivol du signal de réponse en provenance de l'identifiant.

Le graphe de la figure 3 est purement illustratif du principe général de l'invention. Dans la partie supérieure de ce graphe, on a illustré les moments d'émission par la centrale d'antivol 10, d'un signal d'interrogation E et, sur la partie basse du graphe, on a illustré, sur la même échelle de temps, les moments de réception, par la centrale 10, du signal de réponse R.

Bien entendu, la durée, la forme, ainsi que l'espacement dans le temps des différents signaux ne sont ici donnés qu'à titre d'exemples illustratifs destinés à permettre une compréhension simple de l'invention.

Ainsi, on peut voir qu'à l'instant TE(1), la centrale d'antivol 10 commence à émettre un premier signal d'identification. A partir de l'instant TR(1), la centrale d'antivol 10 commence à recevoir un signal de réponse en provenance de l'identifiant 12.

5 L'intervalle de temps  $\Delta T1$  qui sépare l'instant TE(1) de l'instant TR(1) constitue donc une mesure de la durée de la boucle d'identification qui regroupe l'aller d'un signal d'interrogation E et le retour d'un signal de réponse R.

10 Cette durée dépend, dans une faible mesure, de la distance qui sépare réellement la centrale d'antivol de l'identifiant 12 et, pour une plus grande part, du temps de réponse de l'identifiant.

Or, si comme cela est représenté à la figure 2, des relais 14, 16 ont été interposés dans le trajet du signal entre la centrale 10 et l'identifiant 12, cet intervalle de temps  $\Delta T1$  s'en trouvera forcément  
15 augmenté. Cette augmentation résultera là encore, pour une faible part, de l'accroissement de la distance parcourue par les signaux électromagnétiques et, pour une large part, du temps de transfert du signal au travers de chacun des relais 14, 16, tant à l'aller qu'au retour.

20 Ainsi, dans ce cas, le signal est relayé à quatre reprises, ce qui peut entraîner un accroissement de l'intervalle de temps  $\Delta T1$  non négligeable.

Aussi, en comparant l'intervalle de temps  $\Delta T1$  à une durée prédéterminée, la centrale d'antivol 10 peut détecter une anomalie dans l'échange de données entre la centrale 10 et l'identifiant 12 et refuser la  
25 délivrance d'un signal d'autorisation en dépit du fait que le signal reçu en réponse est un signal conforme, c'est-à-dire portant un code authentique.

Cette simple opération de comparaison de la durée de la boucle d'échange de données permet donc de renforcer de manière important le  
30 niveau de sécurité que permet d'obtenir un tel système.

Cependant, le système tel qu'il vient d'être décrit nécessite de mesurer des intervalles de temps particulièrement courts, et il doit être de plus particulièrement précis pour pouvoir comparer ces intervalles de temps à une durée prédéterminée et pour pouvoir détecter une  
35 augmentation de cette durée, due par exemple à la présence de relais, qui risque d'être relativement faible.

Une telle précision peut être la source d'un coût important des dispositifs à mettre en oeuvre.

Aussi, selon un second aspect de l'invention, on a prévu des moyens qui permettent de mettre en oeuvre l'invention tout en utilisant des composants et des circuits électroniques de faible coût.

A cet effet, on prévoit que, à chaque opération d'identification, l'échange de données entre la centrale d'antivol 10 et l'identifiant 12 ne soit pas effectué sous la forme d'une unique boucle d'identification comportant un seul trajet aller-retour du signal, mais sous la forme d'un échange comportant une série de boucles d'identification successives.

Comme on peut le voir sur la figure 3, on choisit de faire ré-  
10 émettre à la centrale d'antivol 10, lorsqu'elle a reçu le premier signal de réponse de l'identifiant 12, un deuxième signal d'identification qui est émis à l'instant TE(2). A ce deuxième signal d'identification, l'identifiant répond par un deuxième signal de réponse qui est reçu par la centrale 10 à l'instant TR(2). On prévoit que l'échange de données comporte  
15 ainsi un nombre entier N de boucles d'identification, la dernière boucle comportant, à l'instant TE(N) l'émission d'un signal d'interrogation et, à l'instant TR(N), la réception d'un  $i$ ème signal de réponse en provenance de l'identifiant 12.

Dans ce dispositif, le signal d'interrogation de la boucle de rang  
20 quelconque K n'est pas émis à un instant qui suit d'une durée fixe l'émission du signal d'interrogation de la boucle de rang K-1. Au contraire, l'émission du signal d'interrogation de la boucle de rang K est effectuée à un instant qui suit d'une durée fixe la réception du signal de réponse de la boucle de rang K-1.

25 De la sorte, lorsque l'on se situe dans le cas de la figure 2, dans lequel des relais 14, 16 sont interposés entre la centrale 10 et l'identifiant 12, le temps perdu dans le signal au niveau de chaque relais 14, 16 se cumule à chaque boucle. Aussi, au bout d'un nombre N de boucles d'identification, ce retard est égal à N fois le retard pris au  
30 cours d'une seule boucle.

En choisissant un nombre important de boucles, par exemple 100 ou 1000, on peut ainsi très facilement augmenter la valeur de ce retard et en rendre la mesure beaucoup plus simple, réalisable à l'aide de circuits électroniques peu onéreux.

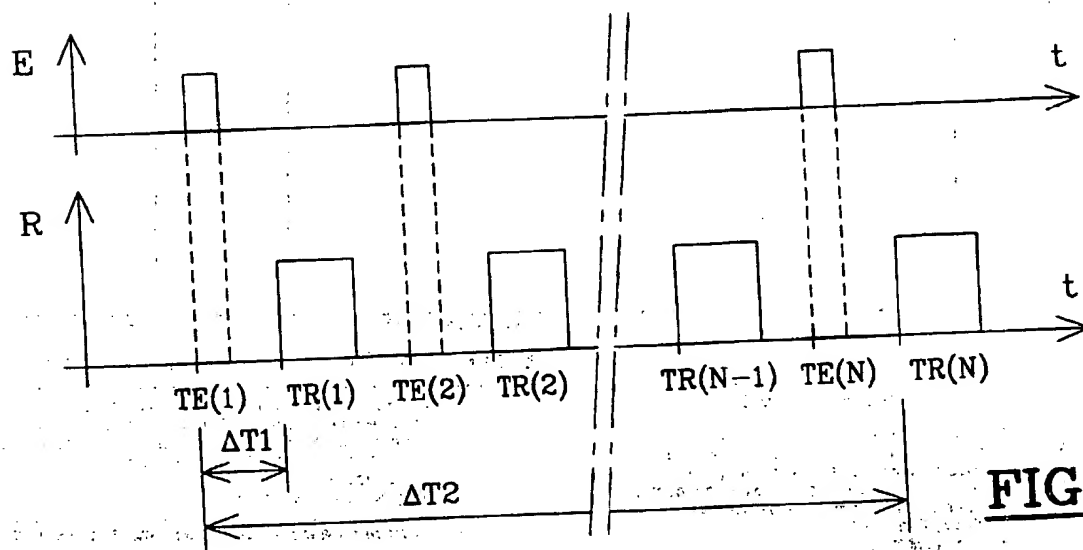
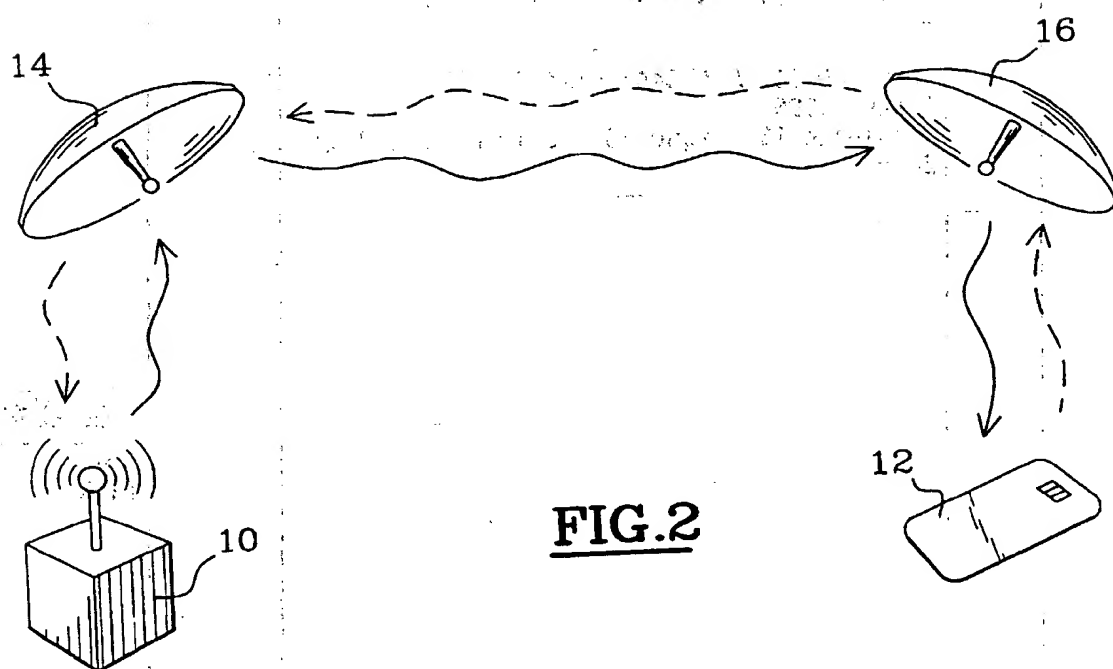
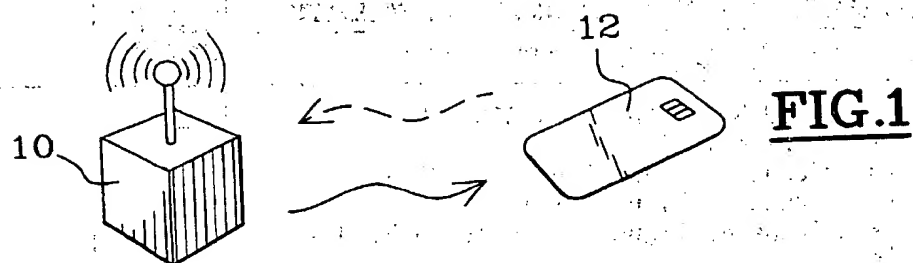
35 Ainsi, comme on l'a représenté sur la figure 3, on pourra par exemple mesurer l'intervalle de temps  $\Delta T_2$  séparant l'instant TE(1) de l'instant TR(N) et comparer cette valeur à une valeur prédéterminée gardée en mémoire par la centrale 10.

Bien entendu, le système de sécurité selon l'invention peut servir à autoriser la décondamnation des serrures d'ouvrant d'un véhicule automobile, mais il peut aussi être utilisé pour autoriser toute autre fonction du véhicule, par exemple l'allumage ou l'injection dans le moteur, le déblocage de la colonne de direction, ou la mise en marche de tout appareil électrique.



**REVENDICATIONS**

1. Système de sécurité pour un véhicule automobile, du type dans lequel, en vue de la délivrance d'une autorisation, le système
- 5 procède à une opération d'identification au moyen de signaux électromagnétiques échangés à distance entre une centrale d'identification (10) et un identifiant (12), du type dans lequel l'opération d'identification comporte une étape d'échange de données au cours de laquelle est exécutée au moins une boucle d'identification selon laquelle
- 10 un signal d'interrogation est émis par la centrale (10) vers l'identifiant (12) qui émet en retour un signal de réponse en direction de la centrale (10), et du type dans lequel l'opération d'identification comporte une étape d'authentification du signal de réponse,
- caractérisé en ce que l'opération d'identification comporte une
- 15 étape de contrôle de la durée de l'étape d'échange de données.
2. Système de sécurité selon la revendication 1, caractérisé en ce que l'étape de contrôle de la durée compare la durée entre l'émission par la centrale d'un signal d'interrogation et la réception par la centrale (10) du signal retour correspondant, avec une durée prédéterminée.
- 20 3. Système de sécurité selon la revendication 2, caractérisé en ce que l'étape d'échange de données comporte l'exécution d'une série de boucles successives d'identification, une boucle de rang supérieur n'étant exécutée qu'une fois achevée la boucle de rang immédiatement inférieur, et en ce que l'étape de contrôle de la durée compare la durée
- 25 entre l'émission du signal d'interrogation d'une boucle de la série et la réception du signal de réponse d'une boucle de rang supérieur déterminé, avec une durée prédéterminée.
4. Système de sécurité selon l'une quelconque des revendications précédentes, caractérisé en ce que les signaux électromagnétiques échangés entre la centrale d'identification et
- 30 l'identifiant sont, dans l'un au moins des sens de transmission, des signaux de faible portée.



2781076

REPUBLIQUE FRANÇAISE


INSTITUT NATIONAL  
de la  
PROPRIETE INDUSTRIELLE

**RAPPORT DE RECHERCHE  
PRELIMINAIRE**

établi sur la base des dernières revendications  
déposées avant le commencement de la recherche

N° d'enregistrement  
national

FA 560142  
FR 9808863

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X	EP 0 823 520 A (DAIMLER BENZ AG) 11 février 1998 * colonne 3, ligne 6 - ligne 21 * * colonne 4, ligne 8 - ligne 23 * * colonne 4, ligne 47 - colonne 5, ligne 1 * * colonne 6, ligne 53 - colonne 7, ligne 45 *	1, 2, 4
A	EP 0 640 517 A (TOKAI RIKI CO LTD) 1 mars 1995 * colonne 13, ligne 35 - colonne 15, ligne 20 *	1, 3
		DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)
		B60R E05B
		
Date d'achèvement de la recherche		Examinateur
16 avril 1999		Areal Calama, A-A
<p><b>CATEGORIE DES DOCUMENTS CITES</b></p> <p>X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général O : divulgation non-écrite P : document intercalaire</p> <p>T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons &amp; : membre de la même famille, document correspondant</p>		

**This Page Blank (uspto,**